UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
X

UNITED STATES OF AMERICA,

v.

DILKHAYOT KASIMOV and
AZIZJON RAKHMATOV,

Defendants.
X

**CASE NO. 15-CR-95**

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTIONS

UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTIONS TO SUPPRESS EVIDENCE OBTAINED OR DERIVED FROM ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND FOR DISCLOSURE OF FISA MATERIALS

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Eastern District of New York and Assistant United States Attorneys Douglas M. Pravda, David K. Kessler and J. Matthew Haggans, hereby files its UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTIONS TO SUPPRESS EVIDENCE OBTAINED OR DERIVED FROM ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND FOR DISCLOSURE OF FISA MATERIALS.

This UNCLASSIFIED MEMORANDUM is based upon the attached memorandum of points and authorities, a sealed appendix, and the files and records in this case.

Dated: August 16, 2019

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

/s/
DOUGLAS M. PRAVDA
DAVID K. KESSLER
J. MATTHEW HAGGANS
Assistant United States Attorneys
Eastern District of New York

/s/
STEVEN WARD
Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice

/s/
PURVI PATEL
Attorney Advisor
Office of Intelligence
National Security Division
United States Department of Justice

Attorneys for Plaintiff
UNITED STATES OF AMERICA

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## FEDERAL CASES

**U.S. CONSTITUTION**



**FEDERAL STATUTES**

**OTHER AUTHORITIES**

## I. INTRODUCTION

The Government is filing this unclassified memorandum in opposition to defendant Dilkhayot Kasimov's ("Kasimov") "Motion to Disclose FISA Materials and Suppress All FISA Evidence" ("Kasimov motion") and defendant Azizjon Rakhmatov's ("Rakhmatov") "Motion for Discovery and Suppression of Electronic Surveillance and Physical Searches Conducted Pursuant to the Foreign Intelligence Surveillance Act and All Evidence and Information Derived Therefrom" ("Rakhmatov motion") (hereinafter, collectively referred to as "defendants' motions"). The defendants' motions seek: (1) suppression of all evidence obtained under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801 *et seq.*, (*i.e.*, "the FISA information"); and (2) disclosure of the FISA applications, orders, and related materials (*i.e.*, "the FISA materials").[1]

The defendants' motions have triggered this Court's review of the materials related to the FISA-authorized[2] electronic surveillance and physical search to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval.[3] Whenever "a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court . . . shall . . . if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the

---

[1] **[CLASSIFIED MATERIAL REDACTED]**

[2] **[CLASSIFIED MATERIAL REDACTED]**

[3] The provisions of FISA that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g). The Government is filing herewith such an affidavit in which the Attorney General claims under oath that disclosure or an adversary hearing would harm the national security of the United States, which is the prerequisite for the Court to review the FISA materials *in camera* and *ex parte*.[4] Consequently, the Government respectfully submits that, for the reasons set forth herein, this Court must conduct an *in camera*, *ex parte* review of the documents relevant to the defendants' motions in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).[5]

For the reasons set forth below and from the Court's *in camera*, *ex parte* review of the FISA materials, it is conclusively established that: (1) the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendants of the FISA materials and the Government's classified submissions is not authorized because the Court can make an accurate determination of the legality of the FISA-authorized electronic surveillance and physical search without disclosing the FISA materials or portions thereof; (3) the FISA materials should not be disclosed; (4) the FISA information should not be suppressed; and (5) no hearing is required.

## A. BACKGROUND

On April 6, 2015, a grand jury in the Eastern District of New York ("EDNY") returned an indictment charging Kasimov, Abdurasul Hasanovich Juraboev ("Juraboev"), Akhror Saidakhmetov ("Saidakhmetov"), and Abror Habibov ("Habibov") with one count of conspiracy, and one count of attempt, to provide material support to a foreign terrorist organization ("FTO"),

[4] The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and attached as part of the Government's classified filing. *See* Sealed Exhibit 1.

[5] **[CLASSIFIED MATERIAL REDACTED]**

in violation of 18 U.S.C. § 2339B. Saidakhmetov and Habibov were additionally charged with one count of conspiracy to use a firearm, in violation of 18 U.S.C. § 924, and Saidakhmetov was charged with one count of travel document fraud, in violation of 18 U.S.C. § 1546(a). (Docket Entry ("Doc.") 28.)

On June 8, 2015, a grand jury in the EDNY returned a superseding indictment charging Kasimov, Juraboev, Saidakhmetov, and Habibov with the same offenses, and charging Akmal Zakirov ("Zakirov") with one count of conspiracy, and one count of attempt, to provide material support to an FTO, in violation of 18 U.S.C. § 2339B. (Doc. 63.)

On May 9, 2016, a grand jury in the EDNY returned a second superseding indictment charging Kasimov, Saidakhmetov, Habibov, and Zakirov with the same offenses, and charging Rakhmatov with one count of conspiracy, and one count of attempt, to provide material support to an FTO, in violation of 18 U.S.C. § 2339B, and one count of conspiracy to use a firearm, in violation of 18 U.S.C. § 924. (Doc. 135.) A trial date has been set for September 16, 2019.[6]

**[CLASSIFIED MATERIAL REDACTED]**

On May 4, 2015, pursuant to 50 U.S.C. § 1806(c), the United States provided notice to Kasimov stating that it "intends to offer into evidence, or otherwise use or disclose in any proceedings in [this case], information obtained or derived from electronic surveillance conducted pursuant to [FISA], as amended, 50 U.S.C. §§ 1801-1812." (Doc. 51.) On September 7, 2017, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Rakhmatov stating that it "intends to offer into evidence, or otherwise use or disclose in any

[6] On August 14, 2015, and January 19, 2017, respectively, Juraboev and Saidakhmetov pleaded guilty to conspiring to provide material support to an FTO, and were each subsequently sentenced to 180 months of incarceration. On August 29, 2017, Habibov pleaded guilty to conspiring to provide material support to an FTO and conspiring to use a firearm. On March 16, 2018, Zakirov pleaded guilty to conspiring and attempting to provide material support to an FTO. Both Habibov and Zakirov are awaiting sentencing.

proceedings in [this case], information obtained or derived from electronic surveillance and physical search conducted pursuant to [FISA], as amended, 50 U.S.C. §§ 1801-1812 and §§ 1821-1829." (Doc. 222.) On July 8, 2019, and July 9, 2019, respectively, Kasimov and Rakhmatov filed the instant motions.[7]

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**[8]

In subsequent sections of this Memorandum, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize the facts supporting the FISC's probable cause determinations at issue (all of which information is contained fully in the exhibits in the Sealed Appendix); (5) discuss the relevant minimization procedures; and (6) address the defendants' arguments in support of their motions. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendants' requests, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct the required *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval; (3) find that the FISA information should not be suppressed; and (4) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

---

[7] Rakhmatov's motion incorporates the motion to suppress FISA information obtained or derived from Titles I and III of FISA, filed in the case of *United States v. Muhtorov*, 12-CR-00033, Doc. No. 125 (D. Colo. May 25, 2012). All citations to the *Muhtorov* attachment will be cited as "Rakhmatov motion attach." The Government notes that the U.S. District Court for the District of Colorado rejected the defendant's motion to suppress. *See Muhtorov*, 12-CR-00033, Doc. No. 196. Rakhmatov also submitted a supplemental motion for suppression of FISA documents and recordings on July 30, 2019.

[8] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

### B. OVERVIEW OF THE FISA AUTHORITIES

**[CLASSIFIED MATERIAL REDACTED]**

#### 1. [CLASSIFIED MATERIAL REDACTED]

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

#### 2. [CLASSIFIED MATERIAL REDACTED]

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

#### 3. [CLASSIFIED MATERIAL REDACTED]

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

#### 4. The FISC's Findings

**[CLASSIFIED MATERIAL REDACTED]**

## II. THE FISA PROCESS

### A. OVERVIEW OF FISA[9]

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court

[9] This memorandum references the statutory language in effect at the time relevant to this matter.

of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[10] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than seven days after the Attorney General authorizes such electronic surveillance [or physical search].

50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[11] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. *See* 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).[12]

---

[10] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[11] **[CLASSIFIED MATERIAL REDACTED]**

## B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical search, or both, within the United States where a significant purpose is the collection of foreign intelligence information.[13] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person[14] is necessary to, the ability of the United States to protect against—
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> > (A) the national defense or the security of the United States; or
> >
> > (B) the conduct of the foreign affairs of the United States.

---

[12] If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance or search must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. *See* 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC shall cause to be served on any U.S. person named in the application, and others in the FISC's discretion, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. *See* 50 U.S.C. § 1806(j); *see also* 50 U.S.C. § 1825(j)(1) (physical search). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. *See* 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

[13] **[CLASSIFIED MATERIAL REDACTED]**

[14] **[CLASSIFIED MATERIAL REDACTED]**

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1821(1), adopting the definitions from 50 U.S.C. § 1801. With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures to be followed;
>
> (5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
>
> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be,

owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. § 1823(a)(1)-(8), (a)(3)(B), (C).

**1. The Certification**

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that—
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 50 U.S.C. § 1823(a)(6).

**2. Minimization Procedures**

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

**[CLASSIFIED MATERIAL REDACTED]**

### 3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical search, or both, before they are presented to the FISC.

## C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical search, or both, only upon finding, among other things, that:

> (1) the application has been made by a "Federal officer" and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power);
> (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search);
>
> (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and
>
> (5) if the target is a United States person, that the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean—

> (1) a foreign government or any component, thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons;
>
> (6) an entity that is directed and controlled by a foreign government or governments; or
>
> (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means—

> (1) any person other than a United States person, who—
>
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
>
> (C) engages in international terrorism or activities in preparation therefore [sic];
>
> (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
>
> (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

> (2) any person who—
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. Aug. 18, 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999); *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. Aug. 14, 2006). The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *See United States v. Turner*, 840 F.3d 336, 340-41 (7th Cir. 2016) (finding probable cause that the target of the FISA collection was an agent of a foreign power); *United States v.*

*Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (concluding that the FISA applications established "probable cause to believe that . . . [the targets] were agents of a foreign power at the time the applications were granted"); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. Jan. 24, 2008) (finding that the FISA collection was lawfully collected and finding specifically, *inter alia*, that "[e]ach application contained facts establishing probable cause to believe that, at the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power . . . ."), *aff'd*, 630 F.3d 102, 129 (2d Cir. 2010); *Global Relief Found. Inc. v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. June 11, 2002) (concluding that "the FISA application established probable cause . . . at the time the search was conducted and the application was granted"), *aff'd*, 315 F.3d 748 (7th Cir. 2002). However, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical search, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
>
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;

(5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and

(6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1) and 2(A); 1824(c)(1) and 2(A).

Under FISA, electronic surveillance or physical search targeting a United States person may be approved for up to ninety days, and those targeting a non-United States person may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to ninety days, and one targeting a non-United States person may be approved for up to one year.[15] 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

## III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used.[16] 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds: (1) that the information was unlawfully acquired; or (2)

[15] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

[16] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2). Rakhmatov and Kasimov are "aggrieved persons" under FISA, and as noted above, were provided with notice of their status as such and of the Government's intent to use FISA-obtained or -derived information against them at trial.

that the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant who has received notice of use of FISA may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical search, *i.e.*, the FISA materials. 50 U.S.C. §§ 1806(f), 1825(g).

### A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and physical search, or both, the district court

> shall, notwithstanding any other law, if the Attorney General files an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[17]

50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, such as has been filed here, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g). Thus, the propriety of the disclosure of any FISA applications or orders to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See Abu-Jihaad*, 630 F.3d at 129; *United States v. Duggan*, 743 F.2d 59,

[17] **[CLASSIFIED MATERIAL REDACTED]**

78 (2d Cir. 1984) (After an *in-camera* review, the court "has the discretion to disclose portions of the documents, under appropriate protective procedures, only if [the judge] decides that such disclosure is 'necessary to make an accurate determination of the legality of the surveillance.'") (quoting 50 U.S.C. §1806(f)); *United States v. Daoud*, 755 F.3d 479, 484 (7th Cir. 2014) ("Unless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction."); *United States v. Omar*, 786 F.3d 1104, 1110-11 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Hamide*, 914 F.2d 1147, 1149-50 (9th Cir. 1990) (upon review of the FISA materials, the Court determined "that [disclosure] is not necessary, to the determination of the legality of the electronic surveillances submitted to the court to disclose those [FISA materials] to the respondants."); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (the court "agree[d] with the district court that there [were] 'no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure' in the case."); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982).

### 1. ***In Camera, Ex Parte* Review Is the Rule**

Federal courts, including the Second Circuit, have repeatedly and consistently held that FISA anticipates that an *ex parte*, *in camera* determination is to be the rule, while "[d]isclosure and an adversary hearing are the exception, occurring *only* when necessary." *Daoud*, 755 F.3d at 481 (finding that "the district judge must, in a non-public ('*in camera*'), nonadversarial ('*ex parte*') proceeding, attempt to determine whether the surveillance was proper."); *see also*

*Duggan*, 743 F.2d at 78;[18] *El-Mezain*, 664 F.3d at 567 ("[D]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule") (citing *Abu-Jihaad*, 630 F.3d at 129); *Belfield*, 692 F.2d at 147; *accord Omar*, 786 F.3d at 1110 (quoting *Isa*, 923 F.2d at 1306); *Rosen*, 447 F. Supp. 2d at 546.

In fact, every court but one (whose decision was subsequently overturned by the Seventh Circuit)[19] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera*, *ex parte* review. *See, e.g.*, *United States. v. Stewart*, 590 F.3d 93 (2d Cir. 2009); *Abu-Jihaad*, 531 F. Supp. 2d at 310, *aff'd*, 630 F.3d at 129-30; *Omar*, 786 F.3d at 1110-11; *El-Mezain*, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury ("In re Grand Jury Proceedings")*, 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials); *Isa*, 923 F.2d at 1306 ("study of the materials leaves no doubt that substantial national security interests required the *in camera*, *ex parte* review, and that the district court properly conducted such a review"); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. Feb. 14, 1997)) (noting "this court

[18] In *Duggan*, the Second Circuit explained that disclosure might be necessary "if the judge's initial review revealed potential irregularities such as 'possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." 743 F.2d at 78 (quoting S. REP. 95-604, pt. 1, at 58 1978 U.S.C.C.A.N., at 3960).

[19] The district court in *United States v. Daoud*, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose, stating, "So clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *Daoud*, 755 F.3d at 485.

knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance"); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. Oct. 24, 1990).

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the instant FISA-authorized electronic surveillance and physical search that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. Aug. 5, 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Feb. 18, 2016) (finding the review of the FISA materials was "relatively straightforward and not complex" such that the court "was able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure") (internal quotations and citations omitted); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. Apr. 17, 2008) (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of a high-ranking FBI official in support of the Attorney General's Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *Ott*, 827 F.2d at 477 ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question.") (emphasis in original); *accord Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial national security interests required the *in camera*, *ex parte* review, and that the district court properly conducted such a review"); *United States v. Medunjanin*, No. 10-CR-19-1, 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012) (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation"); *United States v. Islamic Am. Relief Agency ("IARA")*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009).

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of

information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also Stewart*, 590 F.3d at 128 ("FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. . . For this reason, *ex parte*, *in camera* determination is to be the rule.") (quoting *Duggan*, 743 F.2d at 77); *Daoud*, 755 F.3d at 483 ("Everyone recognizes that privacy is a legally protectable interest, and it is not an interest of private individuals alone. [FISA] is an

attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation."); *ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that 50 U.S.C. § 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

**2. *In Camera, Ex Parte* Review Is Constitutional**

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter. *See, e.g.*, *Stewart*, F.3d 590 at 126 (the Second Circuit has concluded that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information.") (quoting *Duggan*, 743 F. 2d at 73); *Abu-Jihaad*, 630 F.3d at 117; *El-Mezain*, 664 F.3d at 567; *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process); *Belfield*, 692 F.2d at 148-49; *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an *ex parte, in camera* review of FISA materials does not deprive a defendant of due process."); *ACLU Found. of So. Cal.*, 952 F.2d at 465; *Isa*, 923 F.2d at 1306 (upholding the district court's *in camera, ex parte* review as constitutional and stating that the process delineated under FISA "provides even more protection" than defendants receive in other contexts); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. May 17, 2006); *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. Dec. 1, 1982) ("*ex parte, in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendant's fourth amendment rights"); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. June 15, 1982) (a "massive body of pre-FISA

case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis).

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials in order to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. Such *in camera, ex parte* review is the rule in such cases and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate venue in which to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

## B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

In evaluating the legality of the FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(f), 1825(g).

### 1. Standard of Review of Probable Cause

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or afforded due deference, courts in the Second Circuit, including in this District, have afforded due deference to the determinations of the

FISC.[20] *See Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review."); *Stewart*, 590 F.3d at 128; *Hasbajrami*, 2016 WL 1029500, at *13; *United States v. Fishenko*, No. 12-CV-626 (SJ), 2014 WL 4804215, at *3 (E.D.N.Y. Sept. 25, 2014); *cf Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial). The material under review here satisfies either standard of review. *See Omar*, 786 F.3d at 1112 ("[W]e have no hesitation in concluding that probable cause under FISA existed under any standard of review.")

**2. Probable Cause Standard**

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a), 1824(a); *Abu-Jihaad*, 630 F.3d at 130. It is this standard — not the standard applicable to criminal search warrants — that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130-31; *Turner*, 840 F.3d at 340-41 (applying the FISA standard of probable cause rather than the probable cause in a criminal case); *Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power.") (quoting *El-Mezain*, 664 F.3d at 564); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)).

**[CLASSIFIED MATERIAL REDACTED]**

[20] **[CLASSIFIED MATERIAL REDACTED]**

The probable cause threshold which the Government must satisfy before receiving authorization to conduct electronic surveillance or a physical search under FISA complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120 (listing sixteen cases that have ruled FISA does not violate the Fourth Amendment).

The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In *Keith*, the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime;" (2) unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information;" and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith* applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith*. In constructing FISA's framework, Congress addressed *Keith*'s question of whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are

reasonable." *See* S. REP. NO. 95-701, 95th Cong., 2d Sess., at 11-12 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980. Similarly, many courts — including the Second Circuit and the FISC of Review — have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See Duggan*, 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *Damrah*, 412 F.3d at 625 (denying the defendant's claim that FISA's procedures violate the Fourth Amendment); *In re Sealed Case*, 310 F.3d 717, 738, 746 (FISA Ct. Rev. 2002) (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (finding FISA's procedures compatible with the Fourth Amendment); *Cavanagh*, 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); *Warsame*, 547 F. Supp. 2d at 993-94; *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135-41 (D. Mass. Nov. 5, 2007) (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. June 22, 2006) ("Courts uniformly have held that FISA procedures satisfy the Fourth Amendment's reasonableness requirement"); *Falvey*, 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

### 3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subject only to minimal scrutiny by the courts," *Badia*, 827 F.2d at 1463, and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *see also Turner*,

840 F.3d at 342 (finding that "our role 'is not to second-guess the executive branch official's certification'") (quoting *In re Grand Jury Proceedings*, 347 F.3d at 204); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *Rosen*, 447 F. Supp. 2d at 545; *Warsame*, 547 F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.; see also In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Rahman*, 861 F. Supp. at 250.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See United States v. Omar*, No. 09-242, 2012 WL 2357734, at *3 (D. Minn. June 20, 2012), *aff'd*, 786 F.3d 1104 ("the reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing"); *see also Campa*, 529 F.3d at 993 ("in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target") (quoting *Badia*, 827 F.2d at 1463); *United States v. Alwan,* No. 1:11-CR-13, 2012 WL 399154, at *7 (W.D. Ky. Feb. 7, 2012) ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made") (quoting *United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *20 (N.D. Ga. Mar. 19, 2009). Under FISA, "[T]he FISA Judge need only determine that the application contains all of the statements and certifications required by the Act if the target is a non-United States person, whereas he must also find that the certifications are not 'clearly erroneous' if the

target is a United States person." *Duggan*, 743 F.2d at 75;[21] *see also Turner*, 840 F.3d at 342 (the district court "must ensure that the government's certifications are not 'clearly erroneous' when the target is a U.S. person."); *Campa*, 529 F.3d at 994; *United States v. Kashmiri*, No. 09-CR-830, 2010 WL 4705159, at *2 (N.D. Ill. Nov. 10, 2010). A "clearly erroneous" finding is established only when "although there is evidence to support it, the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

**4. FISA Is Subject to the Good Faith Exception**

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).[22] Numerous courts have stated that the good faith exception applies to FISA evidence. *See Ning Wen*, 477 F.3d at 897 (noting that federal officers were entitled to rely in good faith on a FISA warrant); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 ("[t]he FISA evidence obtained . . . would be admissible under *Leon*'s 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant"); *Mubayyid*, 521 F. Supp. 2d at 140 n.12 ("there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the

[21] **[CLASSIFIED MATERIAL REDACTED]**

[22] "[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government's case. . . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation" only in those cases where its application will deter police misconduct. *Duka*, 671 F.3d at 346 (citing *Leon*, 468 U.S. at 918).

FISA orders"); *Marzook*, 435 F. Supp. at 790-91 (holding, in an analogous context, that "the FBI's reliance on the Attorney General's approval under Executive Order No. 12,333 – an order that no court has found unconstitutional – was [] objectively reasonable because that order pertains to foreign intelligence gathering.").

The FISA-authorized electronic surveillance and physical search at issue in this case, authorized by a duly enacted statute and an order issued by a neutral judicial officer, would fall squarely within this good faith exception. There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *see also Massachusetts v. Sheppard*, 468 U.S. 981 (1984); *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance and physical search at issue. *Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to those orders would be admissible under *Leon*'s good faith exception to the exclusionary rule.

## IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

**[CLASSIFIED MATERIAL REDACTED]**

### A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

**[CLASSIFIED MATERIAL REDACTED]**

#### 1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

e. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

*1.* [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

*2.* [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

## B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED]

### 1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

### 2. "A Significant Purpose"

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

### 3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

**[CLASSIFIED MATERIAL REDACTED]**

## C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

This Court's *in camera, ex parte* review of the FISA materials will demonstrate that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval (lawfully conducted). That is, the FISA-obtained or -derived information that will be offered into evidence in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, the SMPs adopted by the Attorney General and approved by the FISC.

### 1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the electronic surveillance and physical search were properly certified and the information was lawfully acquired pursuant to FISA, it must then examine whether the electronic surveillance and physical search were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance and physical search were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. Dec. 5, 2000) ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted" [internal quotation marks omitted]). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. REP. No. 95-1283, 95th Cong., 2d Sess., pt. 1, at 55 (1978)); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *Thomson*, 752 F. Supp. at 81

(noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing H.R. REP. NO. 95-1283, pt. 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing H.R. REP. NO. 95-1283, pt. 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. REP. NO. 95-1283, pt. 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. id.* at 81 (quoting H.R. REP. NO. 95-1283, pt. 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Cf. id.* (quoting H.R. REP. NO. 95-1283, pt. 1, at 59).

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. REP. NO. 95-701, at 39, 1978 U.S.C.C.A.N., at 4008 (quoting *United States v. Bynum*, 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); S. REP. NO. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 4008-09 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could

do to avoid unnecessary intrusion"); *IARA*, 2009 WL 5169536, at *6 (quoting S. REP. NO. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 3990-91).

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See id.* at 1305.

Even if certain communications were not properly minimized, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. Sept. 28, 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is the "evidence which was obtained unlawfully." H.R. REP. NO. 95-1283, pt. 1, at 93. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

*Id.*; *see also Falcone*, 364 F. Supp. at 886-87; *accord Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

### 2. The FISA Information Was Appropriately Minimized

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection discussed herein was lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection discussed herein.

## V. THE COURT SHOULD REJECT THE DEFENDANTS' LEGAL ARGUMENTS

In their motions, the defendants present numerous arguments in support of their request for the suppression of FISA-obtained or -derived evidence and the disclosure of the FISA materials. Their arguments essentially fall into two categories: (1) that the FISA-obtained or -derived evidence should be suppressed for several reasons, including because the application(s) may have contained intentional or reckless material falsehoods or omissions and may not have established probable cause, and the FISA procedural requirements may not have been met; and (2) that disclosure of the FISA materials is both necessary for them to litigate suppression issues, and is required by due process considerations. (*See generally* Rakhmatov motion; Kasimov motion.) For the reasons set forth below and as the Court will see in its *ex parte*, *in camera* review of the FISA materials, these arguments are without merit.

## A. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION

In support of their request for suppression, the defendants claim that the FISA information must be suppressed as the application(s) may have: (1) failed to establish that the targets were agents of a foreign power; (2) included certifications that may have been deficient; (3) contained required minimization procedures that were inadequate or not followed; or (4) contained intentional or reckless falsehoods or omissions. (Rakhmatov motion attach., at 2-3, 10-15; Kasimov motion, at 6.) The defendants also raise constitutional challenges related to the FISA statute. (Rakhmatov motion attach., at 17-27, 30-32; Kasimov motion, at 6.)[23] This Court should deny each of these arguments, for the reasons discussed below.

### 1. The Government Satisfied the Probable Cause Requirement of FISA

First, the defendants allege that the FISA application(s) failed to establish probable cause that they were agents of a foreign power.[24] "Probable cause is more than a bare suspicion, but less than absolute certainty," and in making the probable cause determination, FISA permits a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Rosen*, 447 F. Supp. 2d at 549 (quoting *Mason v. Godinez*, 47 F.3d 852, 855 (7th Cir. 1995), 50 U.S.C. § 1805(b). Furthermore, the FISA probable cause standard "does not necessarily require a showing of an imminent violation of criminal law" because Congress clearly intended a different showing of probable cause for these activities than that applicable to ordinary cases. *Rosen*, 447 F. Supp. 2d at 549 (quoting *In re*

[23] In Rakhmatov's motion, he raises other alleged government misconduct relating to unclassified, non-FISA evidence that he believes should "inform" the court's review of the FISA materials. (Rakhmatov motion, at 2-3.) As the Government will explain in detail in an unclassified opposition to Rakhmatov's multiple motions to suppress evidence, which the Government intends to file on August 16, 2019, in accordance with the Court's pretrial motion schedule, the Government acted lawfully and did not engage in any misconduct, none of which in any event relates to the Government's acquisition of FISA information.

[24] **[CLASSIFIED MATERIAL REDACTED]**

*Sealed Case*, 310 F.3d at 738). As discussed above, courts in the Second Circuit have afforded due deference to the probable cause determinations of the FISC. *See Abu-Jihaad*, 630 F.3d at 130; *Stewart*, 590 F.3d at 128; *cf. Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial); *accord Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Gates*, 462 U.S. at 236). As this Court will see from its review of the FISA materials, the Government plainly satisfied the requirements of FISA.

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

Second, Rakhmatov submits that "foreign intelligence probable cause is not 'probable cause' within the ordinary meaning of the Fourth Amendment." (Rakhmatov motion attach., at 27.) The probable cause threshold which the Government must satisfy before receiving authorization to conduct electronic surveillance or physical search under FISA complies with the Fourth Amendment's reasonableness standard. Rakhmatov's argument that FISA's different probable cause standard violates the Fourth Amendment has been uniformly rejected by federal courts. *See, e.g., Abu-Jihaad,* 630 F.3d at 120 (listing sixteen cases that have ruled FISA does not violate the Fourth Amendment).

As discussed above, *see supra* Section III.B.2, the Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23. In *Keith,* the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime;" (2) unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves

the interrelation of various sources and types of information;" and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith* applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith*. In constructing FISA's framework, Congress addressed *Keith's* question of whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* S. REP. NO. 95-701, at 11-12, 1978 U.S.C.C.A.N., at 3980. Similarly, many courts have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See Duggan,* 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); *In re Sealed Case,* 310 F.3d at 738, 746 (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance).

**2. The Certification(s) Complied with FISA**

The defendants submit that the FISA applications may lack proper certifications, the collection of foreign intelligence information may not have been a "significant purpose" of the collection, and the "necessity requirement" may not have been met. (Rakhmatov motion attach., at 2-3, 10-15; Kasimov motion, at 6.) The defendants further argue that the significant purpose standard is unconstitutional. (Rakhmatov motion attach., at 17-22; Kasimov motion, at 6.)

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

Third, the defendants argue that the "significant purpose" standard of FISA is unconstitutional because the Government "can effect an end-run around the Fourth Amendment merely by asserting a desire to gather foreign intelligence information from the person it intends to prosecute." (Rakhmatov motion attach., at 21; *see also* Kasimov motion, at 6.) As part of the USA PATRIOT Act, Congress amended FISA to require that an Executive Branch official now certify that "a significant purpose" of the requested surveillance was to obtain foreign intelligence information. 18 U.S.C. § 1804(a)(6)(B). The "significant purpose" standard has been repeatedly upheld, including by the Second Circuit. As the Second Circuit observed in *Abu-Jihaad*, "[W]e identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a 'significant purpose' to obtain foreign intelligence information. . . ." 630 F.3d at 131; *see also id.* at 128 (concluding that the standard "is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering. . . ."); *Duka*, 671 F.3d at 343 ("the dispositive issue is whether the 'significant purpose' test is reasonable. . . . We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment.").

**[CLASSIFIED MATERIAL REDACTED]**

**3. <u>The Government Complied with the Minimization Procedures</u>**

**[CLASSIFIED MATERIAL REDACTED]**

**[CLASSIFIED MATERIAL REDACTED]**

**4. *Franks v. Delaware* Does Not Require Suppression of FISA Materials**

The defendants speculate that the FISA materials may contain reckless falsehoods or material omissions in violation of *Franks*, 438 U.S. 154. (Rakhmatov motion attach., at 9; Kasimov motion, at 6-8.) In making such a request, Kasimov concedes that he lacks sufficient information to make a credible showing under *Franks* and therefore seeks disclosure of the FISA materials. (Kasimov motion, at 7.) Based on the relevant case law, this Court should decline to hold such a hearing.

To merit a *Franks* hearing, a defendant must make a "concrete and substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection; to obtain a hearing, a defendant must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *Duggan*, 743 F.2d at 77 n.6 (quoting *Franks*, 438 U.S. at 155-56). A defendant must show that the agent lied or recklessly disregarded the truth with specific evidence in the form of "[a]ffidavits or sworn or otherwise reliable statements of witnesses." *Franks*, 438 U.S. at 171. The *Franks* threshold is not met even by an offer of proof of an impropriety that might have affected the outcome of the probable cause determination, but rather requires one that was "necessary to the finding of probable cause." *United States v. Colkley*, 899 F.2d 297, 301-02 (4th Cir. 1990); *see also United States v. Shnewer*, No. 07-459, 2008 U.S. Dist. LEXIS 112001, at *38 (D. N.J. Aug. 17, 2008) ("[E]ven if the Court were to determine there existed a reckless or intentional falsehood or omission in the FISA application materials, the

evidence obtained still should not be suppressed unless the Court makes the further finding that the falsehood or omission was material to the probable cause determination.").

Only after a defendant makes the requisite showing[25] may the Court conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA application(s) sufficient to warrant suppression of the FISA-obtained or -derived evidence. *Franks*, 438 U.S. at 171. The defendants, however, ignore this burden and merely allege the possibility of such misstatements or omissions.[26] As the Court's review of the FISA materials will demonstrate, no material false statements or omissions exist.

To grant the defendants a *Franks* hearing and to disclose to them the FISA materials would allow them, and defendants in every case, to obtain the FISA materials by merely alleging some impropriety.[27] Disclosing FISA materials to defendants would then become the rule, violating Congress' clear intention, set forth in 50 U.S.C. §§ 1806(f) and 1825(g), that the FISA materials be reviewed *in camera* and *ex parte* in a manner consistent with the realities of modern

---

[25] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *Franks*, 438 U.S. at 171; *Colkley*, 899 F.2d at 300; *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

[26] Rakhmatov alleges that an informant who lived with Juraboev and Saidakhmetov instigated and encouraged "the co-defendants to make specific plans to get money to travel overseas for jihad in Syria," and that the Government may have failed to disclose such information to the FISC. (Rakhmatov motion, at 4.) These claims are without merit. As the Government explained in its unclassified motion to preclude the defendants from raising defenses of "entrapment" and "derivative entrapment," Juraboev and Saidakhmetov formed a plan to travel to Syria to wage jihad prior to the Government introduction of the informant. For instance, in an interview by law enforcement on August 15, 2014, prior to the involvement of the informant, Juraboev confirmed his belief in ISIL's terrorist agenda, including the establishment by force of an Islamic caliphate in Iraq and Syria, and expressed his desire to travel to Syria to engage in violence on behalf of ISIL "if Allah wills." In September 2014, again prior to the involvement of the informant, Juraboev and Saidakhmetov discussed how they could travel to Turkey and then cross the Turkish-Syrian border to enter ISIL-controlled territory. All of that conduct happened prior to the Government's introduction of the informant in September 2014, and the informant therefore did not instigate or entrap any co-defendant to travel to Syria to wage jihad on behalf of ISIL. *See* Gov't Mem. of Law in Support of Motion to Preclude Defenses of Entrapment and Derivative Entrapment, No. 15-CR-95 (WFK), Doc. No. 348, at 1-2.

[27] One court referred to this as "backwards reasoning" in denying a defendant's motion to suppress FISA-derived evidence. *Mihalik*, 11-CR-833(A), Doc. No. 108, at 2 (C.D. Cal. Oct. 3, 2012).

intelligence needs and investigative techniques. Courts have acknowledged that the FISA statute does not envision such disclosure without establishing a basis for it. In *Belfield*, for example, the court noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure." *Belfield*, 692 F.2d at 148.

Courts have rejected other defendants' attempts to force a *Franks* hearing by positing unsupported speculation to challenge the validity of FISC orders, and this Court should do so here. *See Abu-Jihaad*, 531 F. Supp. 2d at 309; *Turner*, 840 F.3d at 341-42 (in reviewing the classified and unclassified record, the Court found that it made "a meaningful effort to confirm the accuracy of the [FISA] application") (quoting *Daoud*, 755 F.3d at 494-95 (Rovner, J. concurring)) (characterizing this review as serving "the same interest . . . that a *Franks* motion serves"); *see also Kashmiri*, 2010 WL 4705159, at *6 (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review"); *Shnewer*, 2008 U.S. Dist. LEXIS 112001, at *37 ("This catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme."); *Mubayyid,* 521 F. Supp. 2d at 131 ("The balance struck under FISA — which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards — would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.").

Here, the defendants have failed to carry the burden of establishing the prerequisites for an adversary hearing, and their attempt to obtain disclosure of the FISA materials to meet that burden is unprecedented and runs counter to FISA, *Franks*, and the intent of Congress. Moreover, the Government respectfully submits that this Court's *in camera*, *ex parte* review of the FISA materials will demonstrate that "an adversary hearing in this case would be academic

because there is no question the FISA applications pass muster." *Medunjanin*, 2012 WL 526428, at *9. For these reasons, the Court should deny the defendants' request for a *Franks* hearing and their request for suppression of the FISA information.

**5. Rakhmatov's Fourth Amendment Challenges Have No Merit**

The defendants argue that the FISA statute violates several Fourth Amendment protections. (Rakhmatov motion attach., at 22-27; Kasimov motion, at 6.) Rakhmatov claims that the suppression process under FISA unconstitutionally interferes with federal courts' Article III judicial power and violates the Constitution's separation of powers by robbing FISA judges of their judicial independence. These arguments fail to reflect the composition and procedures set forth in FISA and have been specifically rejected by other courts. For example, the court in *Megahey* rejected the defendant's constitutional challenge and noted that applications for electronic surveillance submitted to the FISC involve concrete questions respecting the application of FISA and are in such a form that a judge is capable of acting on them, much as he might otherwise act on an *ex parte* application for a warrant. *Megahey*, 553 F. Supp. at 1196. The court also stated that a FISA judge faced with a surveillance application is not called on to issue an advisory opinion, but is instead called on to ensure that the individuals who are targeted do not have their privacy interests invaded, except in compliance with the detailed requirements of the statute. *Id.* at 1197; *see also Falvey*, 540 F. Supp. at 1313, n. 16 (rejecting defendant's argument that a federal district court judge would become a rubber stamp while acting as a FISA judge).

Rakhmatov also claims as a constitutional deficiency of FISA that the Government's FISA applications are not subject to review by a neutral and detached magistrate, as required by the Fourth Amendment. To the contrary, courts have found that Article III judges sitting as judges of the FISC are "neutral and detached" magistrates and provide meaningful judicial

review for purposes of the Fourth Amendment. *Cavanagh*, 807 F.2d at 791 (finding that the FISC provides "neutral and responsible oversight of the government's activities in foreign intelligence surveillance"); *Duka,* 671 F.3d at 337; *Benkahla,* 437 F. Supp. 2d at 554; *Mubayyid*, 521 F. Supp. 2d at 135-41; *United States v. Spanjol*, 720 F. Supp. 55, 58 (E.D. Pa. Aug. 22, 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992); *see also Cavanagh*, 807 F.2d at 790 (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); *Falvey*, 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

Furthermore, Rakhmatov alleges that FISA runs afoul of *Berger's* concern regarding the duration and scope of surveillance: he notes that Title III was drafted shortly after *Berger* was decided and that it limits the term of electronic surveillance orders to 30 days each, whereas FISA permits surveillance for longer time periods. (Rakhmatov motion attach., at 26.) However, it is significant that the defendant fails to mention that *Berger* provided for 60 day periods of surveillance with no provision for terminating that surveillance earlier when its objectives had been obtained. *Berger v. New York*, 388 U.S. 41, 59-60 (1967). To the contrary, FISA requires that electronic surveillance of United States persons terminate once the surveillance has achieved its purpose. 50 U.S.C. § 1805(d)(1). Furthermore, the need for the longer period of surveillance appropriate to the special nature of FISA surveillance was affirmed in *Sealed Case*, 310 F.3d. at 740. In that case, the FISC of Review differentiated between the durations of criminal wiretaps and FISA "based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information'". 310 F.3d at 740 (quoting *Keith*, 407 U.S. at 322).

Rakhmatov's assertions of a number of disparate arguments that FISA violates the Fourth Amendment do not give those arguments any additional weight:

> arguments that FISA violates the Fourth Amendment's requirements of a neutral and detached magistrate, a warrant supported by probable cause, particularity, timely information, and notice have been rejected by the courts. . . . *See, e.g., Abu-Jihaad*, 630 F.3d at 123; *Hammoud*, 381 F.3d at 334; *Benkahla,* 437 F. Supp. 2d at 541, 554. As such, the court will not engage in a lengthy discussion regarding these issues.

*Sherifi,* 793 F. Supp. 2d at 759-60. Indeed, "[e]very court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *30 (order denying defendants' motion to disclose and suppress FISA materials). Accordingly, the Government respectfully submits that this Court should also reject the defendants' meritless and unsupported constitutional challenges to FISA.[28]

## B. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR THE COURT TO DISCLOSE FISA MATERIALS

In support of their arguments for disclosure of the FISA materials, the defendants claim that disclosure: (1) may be necessary under 50 U.S.C. § 1806(f); (2) is required under 50 U.S.C. § 1806(g) and due process; and (3) is required under the Sixth Amendment. (Rakhmatov motion attach., at 9, 15-17, 28-29; Kasimov motion, at 4-5.) For the following reasons, the Court should deny the request for disclosure.

### 1. Disclosure Is Not "Necessary" Under FISA

The defendants request disclosure pursuant to 50 U.S.C. § 1806(f). (Rakhmatov motion attach., at 9; Kasimov motion, at 4-5.) 50 U.S.C. § 1806(f) provides that "the court may disclose . . . portions of the application, order or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Rakhmatov argues that "there are many potential bases for suppression based on unlawful surveillance" and "several complicated issues that make the defense's input necessary."

[28] **[CLASSIFIED MATERIAL REDACTED]**

(Rakhmatov motion attach., at 9.) Kasimov states that "FISA's methodology concerning discovery and requiring motions to suppress FISA-acquired evidence to be prematurely-filed presents an archetypal chicken-and-egg conundrum." (Kasimov motion, at 5.) As the Court is aware, these claims are not unique to this case, and, as detailed above, the defendants have already raised such potential grounds in support of suppression. The defendants, then, are seeking disclosure to bolster their arguments for suppression, which is not permissible under the statute.

Disclosure of the FISA materials to defense counsel is authorized only in one set of circumstances: The Court must conduct its review of FISA materials *in camera* and *ex parte*, and disclosure is within the Court's discretion only following that review and only if the Court is unable to determine the legality of the electronic surveillance, physical search, or both, without the assistance of defense counsel. 50 U.S.C. §§ 1806(f), 1825(g); *Duggan*, 743 F.2d at 78; *Daoud*, 755 F.3d at 482; *In re Grand Jury Proceedings*, 347 F.3d at 203; *Rosen*, 447 F. Supp. 2d at 546. This holding is fully supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." S. REP. NO. 95-701, at 64-65, 1978 U.S.C.C.A.N., at 4034. As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without input from defense counsel.[29]

[29] Even where defendants have alleged specific errors or misrepresentations in the FISA applications, based on their analysis of the evidence in the case, courts have deemed disclosure unnecessary because they were able to rule on the legality of the surveillance, even in light of the alleged errors, through *in camera, ex parte* review. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 130; *United States v. Rosen*, 447 F. Supp. 2d at 552 (denying disclosure despite minimization errors that were inadvertent, disclosed to the FISC, and promptly rectified).

The defendants' request, which effectively calls for disclosure where defense counsel could provide assistance, instead of where necessary, is merely an attempt to circumvent the clear language of the statute. *See* 50 U.S.C. §§ 1806(f), 1825(g). As the *Belfield* court stated: "Congress was adamant, in enacting FISA, that [its] 'carefully drawn procedure[s]' are not to be bypassed." 692 F.2d at 146 (citing S. REP. NO. 95-701, at 63); *see also United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *32 (D. Or. June 24, 2014) ("Obviously it would be helpful to the court to have defense counsel review the materials prior to making arguments. Congress, however, did not put 'helpful' in the statute; it chose 'necessary.'"). As the *Daoud* court stated, "the defendant's misreading of the statute" would circumvent the required *in camera, ex parte* review whenever a defense counsel "believed disclosure necessary, since if the judge does not conduct the *ex parte* review, she will have no basis for doubting the lawyer's claim of necessity." 755 F.3d at 482.

The defendants are not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10. *See also Badia*, 827 F.2d at 1464 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors"); *Mubayyid*, 521 F. Supp. 2d at 131.

The defendants have failed to present any colorable basis for disclosure, as this Court is able to review and make a determination as to the legality of the FISA collection without the assistance of defense counsel. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress' clear intention is

that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is simply nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 ("exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively") (citing *Belfield*, 692 F.2d at 147).

**2. Due Process and Other Constitutional Provisions Do Not Require Disclosure**

Rakhmatov also claims that he is entitled to disclosure of the FISA materials under 50 U.S.C. § 1806(g) and the Due Process Clause of the Fifth Amendment. (Rakhmatov motion attach., at 15-17.) Courts are in agreement, however, that FISA's *in camera*, *ex parte* review does not violate due process, nor does due process require that the defendant be granted access to the FISA materials except as provided for in 50 U.S.C. §§ 1806(f), (g) and 1825(g), (h). *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 117; *El-Mezain*, 664 F.3d at 567; *Damrah*, 412 F.3d at 624; *ACLU Found. of So. Cal*, 952 F.2d at 465; *Ott*, 827 F.2d at 476-77; *Belfield*, 692 F.2d at 148-49.

Nevertheless, Rakhmatov appears to be arguing for disclosure under the balancing test applied by the Supreme Court in *Mathews v. Eldridge*, 424 U.S. 319 (1976), which requires consideration of: (1) the defendant's private interest in disclosure of the materials; (2) the risk that the defendant will be erroneously deprived of his right to the materials; and (3) the Government's interest in preventing disclosure of the materials. 424 U.S. at 335; *see also El-Mezain*, 664 F.3d at 567. According to the defendant, "[i]n a contest between disclosure of state secrets and the defendant's right to a fair trial, the latter wins out." (Rakhmatov motion attach., at 15.) The defendant's claim fails, however, because "it is inappropriate to employ the *Mathews* balancing test in criminal cases." *Hines v. Miller*, 318 F.3d 157, 161 (2d Cir. 2003).

The Supreme Court has questioned the appropriateness of the *Mathews* balancing test for analyzing due process claims in criminal cases. In *Medina v. California*, 505 U.S. 437 (1992), the Court stated that "the *Mathews* balancing test does not provide the appropriate framework for assessing the validity of state procedural rules which, like the one at bar, are part of the criminal process." *Id.* at 443. The Court explained that:

> [i]n the field of criminal law, we "have defined the category of infractions that violate 'fundamental fairness' very narrowly" based on the recognition that, "[b]eyond the specific guarantees enumerated in the Bill of Rights, the Due Process Clause has limited operation." The Bill of Rights speaks in explicit terms to many aspects of criminal procedure, and the expansion of those constitutional guarantees under the open-ended rubric of the Due Process Clause invites undue interference with both considered legislative judgments and the careful balance that the Constitution strikes between liberty and order.

*Id.* (internal citations omitted). The Court observed that it had "invoked *Mathews* in resolving due process claims in criminal law cases on only two occasions," in *United States v. Raddatz*, 447 U.S. 667 (1980), and *Ake v. Oklahoma*, 470 U.S. 68 (1985), and "it is not at all clear that *Mathews* was essential to the results in those cases." *Medina*, 505 U.S. at 444. The decision in *Mathews*, therefore, identifies no due process right that requires disclosure of FISA materials to the defendant, and this Court should decline his invitation to use an inappropriate analytical framework to do so.

Because of the questionable application of the *Mathews* balancing test to due process claims in criminal cases, federal courts have been reticent to apply it to the disclosure of FISA materials. *See, e.g.*, *El-Mezain*, 664 F.3d at 567 ("[a]ssuming without deciding that that the *Mathews* balancing test is applicable"); *Warsame*, 547 F. Supp. 2d at 988 (court "not convinced that *Mathews* balancing test supplies an appropriate framework for evaluating FISA procedures"); *Damrah*, 412 F.3d at 624 (stating that defendant's "reliance on *Mathews* is misplaced . . . because FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process"). As discussed below,

those courts that have applied the test have consistently found that the three factors weigh in favor of the *ex parte*, *in camera* determination of legality required by FISA and against disclosure of the FISA materials.

In *Warsame*, the court acknowledged the defendant's important privacy and liberty interests, and held that disclosure of the FISA materials was not "the appropriate response to this concern." 547 F. Supp. 2d at 988. The court stated that "FISA attempts to protect the rights of individuals not through mandatory disclosure but through 'in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.'" *Id.* at 988-89 (quoting *Belfield*, 692 F.2d at 148). The court found that, given these protections, and the court's careful review of the FISA materials in the case, "the probable value of disclosure, as well as the risk of nondisclosure, of the FISA materials to the defense [was] low." *Warsame*, 547 F. Supp. 2d at 989. Moreover, the court concluded that the Government "has a substantial national security interest in preventing the disclosure of [the FISA materials]." *Id.*

Similarly, in *El-Mezain*, the Fifth Circuit agreed with the district court's assessment that "the *in camera* and *ex parte* review by the district court adequately ensured that the defendants' statutory and constitutional rights were not violated," and that "as a matter of national security, the Government [had] a substantial interest in maintaining the secrecy of the materials." 664 F.3d at 567. The court noted that "[t]his interest extends not only to the contents of the materials but also to the appearance of confidentiality in the operation of the intelligence services." *Id.* at 567-68 (citing *Sims*, 471 U.S. at 175) ("If potentially valuable intelligence sources come to think that the Agency will be unable to maintain confidentiality of its relationship to them, many could well refuse to supply information to the Agency in the first place.") Thus, even under the

*Mathews* test, the Government's interest outweighs the defendant's interest in disclosure, consistent with the *El-Mezain* and *Warsame* decisions.

In addition, Rakhmatov argues that *ex parte* proceedings would "violate his Fifth and Sixth Amendment rights." (Rakhmatov motion attach., at 28.) This claim is contrary to all of the relevant case law. Several courts have addressed the right to confrontation in this context and found that "FISA's *in camera* review provisions have been held to be constitutional." *United States v. Nicholson*, No. 09-CR-40, 2010 WL 1641167, at *3 (D. Or. Apr. 21, 2010) (citing *Isa*, 923 F.2d at 1307-08) (Sixth Amendment right of confrontation is not violated by FISA's *in camera* review procedure); *see also United States v. Hussein*, No. 13-CR-1514-JM, 2014 WL 1682845, at *3 (S.D. Cal. Apr. 29, 2014) (the "*in camera*, *ex parte* review process under FISA satisfies due process under the United States Constitution."); *United States v. Lahiji*, No. 3:10-506-KI, 2013 WL 550492, at *4 (D. Or. Feb. 12, 2013) (Court found no violation of defendants' Fourth, Fifth, or Sixth Amendment rights); *Benkahla*, 437 F. Supp. 2d at 554; *Nicholson*, 955 F. Supp. at 592 ("Based on the unanimous holdings of prior case law, . . . FISA does not violate . . . the Sixth Amendment[] by authorizing *ex parte in camera* review."); *Falvey*, 540 F. Supp. at 1315-16 (rejecting First, Fifth, and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law of the Supreme Court, Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera*, *ex parte* basis).

Courts have also consistently rejected similar arguments challenging FISA under the Sixth Amendment. *See Isa*, 923 F.2d at 1306-07; *Belfield*, 692 F.2d at 148; *Lahiji*, 2013 WL 550492, at *4; *Warsame*, 547 F. Supp. 2d at 988 n.4 (finding argument "without merit") (citing *Nicholson*, 955 F. Supp. at 592); *Megahey*, 553 F. Supp. at 1193. In overturning a district court's order to disclose FISA materials to the defense, the *Daoud* court described the belief that

"adversary procedure is always essential to resolve contested issues of fact" as "an incomplete description of the American legal system in general and the federal judicial system in particular." 755 F.3d at 482.

Rakhmatov also states that "where state secrets are expected to be elicited from the government, the proper procedure is to follow [the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3]. . . ." (Rakhmatov motion attach., at 16.) The Government's response is based on the statutory language of FISA and the opinions of courts that have addressed motions to disclose FISA materials and to suppress FISA collection. CIPA addresses pretrial discovery of classified information by defendants, and procedures to safeguard classified information, both before and during trial, that is either not discoverable or not helpful and material to the defense. *See Abu-Jihaad*, 630 F.3d at 141. CIPA provides a separate and distinct statutory framework that is simply inapplicable to this motion seeking disclosure of FISA materials, which is governed by 50 U.S.C. §§ 1806 and 1825. For these reasons, the *Mathews* decision lends no support to the defendant's claim that due process requires disclosure of the FISA materials.

The plain intention of 50 U.S.C §§ 1806(g) and 1825(h) — allowing the Court to order disclosure of material to which the defendant would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady v. Maryland*, 373 U.S. 83 (1963), even while ruling against the defendant's motion generally — cannot be interpreted to support Rakhmatov's demand for access to all of the FISA materials in advance of the Court's *in camera*, *ex parte* review and determination of the legality of the collection. With respect to any claim that the FISA materials contain information that due process requires be disclosed to the defense, the request is premature since the Court will make that factual determination for itself during its *in camera*, *ex parte* review. The Government is confident that the Court's review of

the challenged FISA materials will not reveal any material that due process requires be disclosed to the defendant, such as *Brady* material, as provided for in 50 U.S.C. § 1806(g). Accordingly, Rakhmatov's claim that he is entitled to the disclosure of the FISA material under 50 U.S.C. § 1806(g) and due process should be rejected.

The defendants' arguments in support of disclosure of the FISA materials have no basis in the law, and disclosure of the FISA materials would cause exceptionally grave damage to the national security. The Government respectfully submits that there is nothing extraordinary about this case to justify an order to disclose the highly sensitive and classified FISA materials in this case under the applicable FISA standard. *See Rosen*, 477 F. Supp. 2d at 546 ("Review of the FISA applications, orders and other materials in this case presented none of the concerns that might warrant disclosure to the defense."). Accordingly, the defendants' motions for disclosure of the FISA materials should be denied.

## VI. RAKHMATOV'S MOTION FOR ADDITIONAL NOTICE AND DISCOVERY SHOULD ALSO BE DENIED

Rakhmatov also seeks "discovery of specific evidence and information and how it was obtained." (Rakhmatov motion, at 1.) As the Court will see from its *in camera*, *ex parte* review of the FISA materials, and for the reasons stated below, the government has complied with its notice and discovery obligations, and thus, Rakhmatov's motion lacks merit and should be denied.

The Government's discovery obligations in a criminal case are not limitless. *See United States v. Agurs*, 427 U.S. 97, 106 (1976) (the Government is under "no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor"); *United States v. Phillips*, 854 F.2d 273, 277 (7th Cir. 1988) (finding that discovery rules do "not grant criminal defendants unfettered access to government files"); *United States v. Griebel,* 312 F. App'x 93, 96 (10th Cir. 2008) (the Government's discovery obligations "are defined by Rule 16, *Brady*,

*Giglio*, and the Jencks Act"). Further, there is no rule of discovery that requires the Government to provide a defendant with a clear, concise narrative regarding the origins of the criminal investigation that led to his arrest. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987) ("defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [Government's] files"); *United States v. Bagley*, 473 U.S. 667, 675 (1985) ("the prosecutor is not required to deliver his entire file to defense counsel"). Rather, the Government is required to provide the defense with all discoverable material (including exculpatory information) described in FED. R. CRIM. P. 16.

Notice concerning the Government's intent to use evidence in a criminal case is generally governed by FED. R. CRIM. P. 12 and 16. FED. R. CRIM. P. 12(b)(4)(B) provides in relevant part: "[T]he defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16." The purpose of this rule is to "provide the defendant with sufficient information to file the necessary suppression motions." *United States v. Ishak*, 277 F.R.D. 156, 158 (E.D. Va. Sept. 9, 2011). "Thus, the government's obligation under Rule 12(b)(4)(B) ends when it has made disclosures that sufficiently allow the defendants to make informed decisions whether to file one or more motions to suppress." *Id.* The Government has satisfied this obligation and provided the defendants with sufficient information and notice to file any necessary motions to suppress. No court has interpreted FED. R. CRIM. P. 12(b)(4)(B) to require the Government to give an accounting of every investigative technique used in the case, regardless of its relationship to admissible evidence. In a criminal case, defense counsel analyzes the discovery, determines what suppression motions to make, and files them. The Government then responds. That is

precisely what has occurred in the instant case. For these reasons, Rakhmatov's request for more information than any rule or statute requires should be denied.

The FISA statute governs the Government's notice obligations with respect to the use of FISA information. The Government's notice obligations regarding the use of FISA information under 50 U.S.C. §§ 1806(c) and 1825(d) apply only if the Government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing, or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. §§ 1806(c), 1825(d). Where all five criteria are met, the Government will notify the defendant and the Court or other authority in which the information is to be used or disclosed that the United States intends to use or disclose such information. On May 4, 2015, pursuant to 50 U.S.C. § 1806(c), the United States provided notice to Kasimov stating that it "intends to offer into evidence, or otherwise use or disclose in any proceedings in [this case], information obtained or derived from electronic surveillance and physical search conducted pursuant to [FISA], as amended, 50 U.S.C. §§ 1801-1812." (Doc. 51) On September 7, 2017, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Rakhmatov stating that it "intends to offer into evidence, or otherwise use or disclose in any proceedings in [this case], information obtained or derived from electronic surveillance and physical search conducted pursuant to [FISA], as amended, 50 U.S.C. §§ 1801-1812 and §§ 1821-1829." (Doc. 222) The Government's notice gave the defendants all the information to which they were entitled and that was necessary to file a motion to suppress.

In the context of FISA collection, Congress has made a decision to allow for greater protection of information than is normally afforded because of the need to protect sensitive national security information, which includes classified sources and methods. Congress intended

that FISA "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." *See* S. REP. NO. 95-701, at 16, 1978 U.S.C.C.A.N., at 3985. As such, in recognition of "the nature of the national interests implicated in matters involving a foreign power or its agents," Congress provided for more limited disclosure than is ordinarily provided with regard to criminal evidence. *Belfield*, 692 F.2d at 148.

Rakhmatov's position that he is entitled to more information regarding FISA-authorized collection is further refuted by the fact that Congress did provide for broader notice of FISA surveillance in certain situations, but declined to do so in the notice sections applicable to criminal defendants. *See Dean v. United States*, 556 U.S. 568, 573 (2009) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."). Specifically, Congress identified three scenarios where more specific notice regarding FISA surveillance was warranted. *See* 50 U.S.C. § 1806(j) (notice of particular information regarding surveillance required where the Attorney General approves emergency surveillance and the Government does not later obtain authorization from the FISC); 50 U.S.C. § 1825(b) (requiring notice identifying property seized, altered, or reproduced during physical search of a U.S. person's residence where the Attorney General has determined that there is no national security interest in continued secrecy); 50 U.S.C. § 1825(j) (notice of particular information regarding physical search required where the Attorney General approves emergency physical search and the Government does not later obtain authorization from the FISC). Congress elected not to require such broad disclosure in the situation where a defendant is charged in a criminal proceeding. *See* 50 U.S.C. §§ 1806(c), 1825(d) (requiring only notice that "the United States intends" to use or disclose FISA-obtained or -derived information).

For the foregoing reasons, the Court should deny Rakhmatov's motion for notice and discovery.

## VII. CONCLUSION

Therefore, for the foregoing reasons, the defendants' motions to disclose the FISA materials and for suppression of the FISA information should be denied. FISA's provisions for *in camera*, *ex parte* review comport with the due process requirements of the United States Constitution. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120; *El-Mezain*, 664 F.3d at 567; *Damrah*, 412 F.3d at 624; *Spanjol*, 720 F. Supp. at 58-59. The defendants advance no argument to justify any deviation from these well-established precedents.

The Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera*, *ex parte* review of the challenged FISA materials to determine whether the information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g). Congress, in enacting FISA's procedures for *in camera*, *ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendants. The FISA materials at issue here are organized and readily understood, and an overview of them has been

presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera*, *ex parte* review, and the defendants have failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

Furthermore, the Court's examination of the FISA materials in the Sealed Appendix will demonstrate that the Government satisfied FISA's requirements to obtain orders for electronic surveillance and physical search, that the information obtained pursuant to FISA was lawfully acquired, and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

Even if this Court were to determine that the acquisition of the FISA information had not been lawfully acquired or that the electronic surveillance and physical search were not made in conformity with an order of authorization or approval, the FISA evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897 (1984). *See also Ning Wen*, 477 F.3d at 897 (holding that the *Leon* good-faith exception applies to FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8.

Based on the foregoing analysis, the Government respectfully submits that the Court must conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submission, and should: (1) find that the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted; (2) hold that disclosure of the FISA materials and the Government's classified submissions to the defendants is not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of electronic surveillance and physical search should not be suppressed; (4) deny the defendants' motions without an evidentiary hearing; and (5) order that the FISA materials and the

Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.

Finally, a district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that the electronic surveillance or physical search was not lawfully authorized or conducted, or an order requiring the disclosure of FISA materials, is each a final order for purposes of appeal. 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, and that the Court stay any such order pending an appeal by the United States of that order.

*****The rest of the page is intentionally left blank*****

Dated: August 16, 2019

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

/s/
DOUGLAS M. PRAVDA
DAVID K. KESSLER
J. MATTHEW HAGGANS
Assistant United States Attorneys
Eastern District of New York

/s/
STEVEN WARD
Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice

/s/
PURVI PATEL
Attorney Advisor
Office of Intelligence
National Security Division
United States Department of Justice

Attorneys for Plaintiff
UNITED STATES OF AMERICA